



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/552,878	04/20/2000	Mark Longworth	MAN0002-US	5009
7590	04/18/2005		EXAMINER	
Brett C. Martin 1650 Tysons Boulevard McLean, VA 22102			EL CHANTI, HUSSEIN A	
			ART UNIT	PAPER NUMBER
			2157	
			DATE MAILED: 04/18/2005	

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/552,878	ABROMAVAGE ET AL.
	Examiner	Art Unit
	Hussein A El-chanti	2157

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 13 October 2004.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-7,9-11,13,14,16-18,20-34,36-38 and 40-54 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-7,9-11,13,14,16-18,20-34,36-38 and 40-54 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 13 October 2004 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: _____.

DETAILED ACTION

1. This action is responsive to amendment received on Oct. 13, 2004. Claims 8, 12, 15, 19, 35 and 39 were canceled. Claims 1, 9, 10, 13, 14, 169 20, 21, 28, 36, 37, 40-43, 45-53 were amended. Claims 1-7, 9-11, 13-14, 16-18, 20-34, 36-38 and 40-54 are pending examination.

Drawings

2. The amended drawings include Fig. 1. Fig. 2-4 were not submitted, Official drawings are required to be submitted by the applicant.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-7, 9-11, 13-14, 16-18, 20-34, 36-38 and 40-54 are rejected under 35 U.S.C. 102(e) as being anticipated by Esbensen, U.S. Patent No. 5,796,942.

Esbensen teaches a system and method for scanning packets sent on a network and in response to detecting a trigger in the packets, the session is reassembled and duplicated (see abstract).

As to claims 1 and 28, Esbensen teaches a system and method respectively for extracting information from network data, comprising:

an input interface connected to at least one source of network data (see col. 4 lines 19-27, packets are scanned and stored for surveillance); and

a network event sensor (see col. 5 lines 14-28, scanner detects a trigger in the received packets), communicating with the input interface , the network event sensor comprising:

an interpreter module, the interpreter module scanning the network data to generate logical groupings of the network data (see col. 3 lines 60-col. 4 lines 5, packets are scanned and stored in a database for testing a set of rules); and

an assembler module communicating with the interpreter module, the assembler module scanning the logical groupings to generate at least one session object (see col. 4 lines 60-67, scanner reconstructs sessions using the stored packets);

wherein the network event sensor applies a lexical engine to the at least one session object to identify the at least one network event as at least one of a predetermined set of event types (see col. 5 lines 14-28, the session is reassembled and scanned for triggers such as name, location, or a login name).

As to claims 2 and 29, Esbensen teaches the system and method of claims 1 and 28 respectively, wherein the at least one source of network data comprises an observation port connected to a network and continuously capturing network data from the network (see col. 4 lines 45-59).

As to claims 3 and 30, Esbensen teaches the system and method of claims 2 and 28 respectively, wherein the observation port comprises a network interface card (see col. 5 lines 15-28).

Art Unit: 2157

As to claims 4 and 31, Esbensen teaches the system and method of claims 3 and 28 respectively, wherein the network comprises at least one of an Ethernet network, a token ring network, and a TCP/IP network (see col. 5 lines 15-28).

As to claims 5 and 32, Esbensen teaches the system and method of claims 3 and 28 respectively, wherein the network interface card is invisible to the network (see col. 5 lines 15-28).

As to claims 6 and 33, Esbensen teaches the system and method of claims 1 and 28 respectively, wherein the at least one source of network data comprises stored network data (see col. 4 lines 35-55).

As to claims 7 and 34, Esbensen teaches the system and method of claims 6 and 28 respectively, wherein the stored network data comprise at least one of captured network files, Website mirrors, archives of Usenet files, and archives of email files (see col. 5 lines 15-28).

As to claims 9 and 36, Esbensen teaches the system and method of claims 8 and 28 respectively, wherein the logical groupings comprise packets (see col. 4 lines 35-55).

As to claims 10 and 37, Esbensen teaches the system and method of claims 8 and 28 respectively, wherein the interpreter module removes low level encoding information from the network data to generate the logical groupings (see col. 5 lines 15-28).

Art Unit: 2157

As to claims 11 and 38, Esbensen teaches the system and method of claims 10 and 28 respectively wherein the low-level encoding information removed by the interpreter module comprises hardware addressing information (see col. 5 lines 15-28).

As to claims 13 and 40, Esbensen teaches the system and method of claims 12 and 28 respectively, wherein the at least one session object comprises at least one session file (see col. 5 lines 15-28).

As to claim 14, Esbensen teaches the system and method of claims 12 and 28 respectively, wherein the assembler module scans the logical groupings by examining at least one of source address, destination address, sequence numbers, source port, and destination port to generate the at least one session object (see col. 5 lines 15-28).

As to claims 16 and 43, Esbensen teaches the system and method of claims 1 and 28 respectively wherein the lexical engine detects the presence of at least one predefined keyword to identify the at least one of a predetermined set of events (see col. 5 lines 15-28).

As to claims 17 and 44, Esbensen teaches the system and method of claims 16 and 28 respectively comprises mail (see col. 5 lines 38-50).

As to claims 18 and 45, Esbensen teaches the system and method of claims 18 and 28 respectively wherein the lexical engine accumulates a total number of occurrences for the at least one predefined keyword (see col. 5 lines 15-55).

As to claims 19 and 46, Esbensen teaches the system and method of claims 18 and 28 respectively wherein the lexical engine applies a threshold to the number of occurrences to identify the event type (see col. 5 lines 15-55).

Art Unit: 2157

As to claims 20 and 47, Esbensen teaches the system and method of claims 12 and 28 respectively, wherein the network event sensor applies the lexical engine recursively to identify more than one event type contained in the at least one session object (see col. 5 lines 15-55).

As to claims 21 and 48, Esbensen teaches the system and method of claims 15 and 28 respectively, further comprising an extractor module, the extractor module extracting the at least one network event from the at least one session object according to the at least one of a predetermined set of event types (see col. 5 lines 15-55).

As to claims 22 and 49, Esbensen teaches the system and method of claims 21 and 28 respectively, wherein the extractor module comprises a library of extractor types, each of the extractor types corresponding to at least one of the at least one of a predetermined set of event types (see col. 5 lines 15-55).

As to claims 23 and 50, Esbensen teaches the system and method of claims 22 and 28 respectively, wherein the extractor module stores a minimum subset of the network data to reconstruct the at least one network event (see col. 7 lines 33-65).

As to claims 24 and 51, Esbensen teaches the system and method of claims 23 and 28 respectively, wherein the minimum subset of the network data is stored in a database (see col. 4 lines 41-55).

As to claims 25 and 52, Esbensen teaches the system and method of claims 24 and 28 respectively, further comprising a presentation module, communicating with the database, the presentation module querying the database for information related to the at least one network event (see col. 4 lines 33-65).

As to claims 26 and 53, Esbensen teaches the system and method of claims 1 and 28 respectively, wherein the network event sensor also applies a port detection engine to the network data to identify the at least one network event (see col. 5 lines 15-55).

As to claims 27 and 54, Esbensen teaches the system and method of claims 1 and 28 respectively, wherein the at least one source of network data comprises a plurality of sources of network data (see col. 5 lines 15-55).

4. Applicant's arguments with respect to the pending claims have been considered but are moot in view of the new grounds of rejection.

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- IRC name translation protocol by Bunny et al., U.S. Patent No. 6,446,112
- Communication management system for a chat system by Okada et al., U.S. patent No. 6,393,461
- Communication management system for computer network-based telephones by Bar et al., U.S. patent No. 6,122,665
- Graphical user interface for Web enabled applications by Bladow et al., U.S. patent No. 6,115,040
- System and method for displaying an electronic mail containing a keyword detected in a chat session message by Murakami, U.S. patent No. 5,987,503
- Interest-based collaborative framework by Aditham, U.S. Patent No. 5,941,945

Art Unit: 2157

- Method and apparatus for providing shared data to a requesting client by Carino, U.S. Patent No. 5,930,786
- Object-oriented system, method and article of manufacture for a client-server session manager in an enterprise computing framework system by Gish, U.S. Patent No. 5,848,246

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

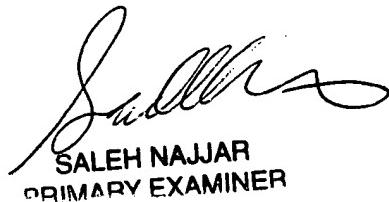
7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hussein A El-chanti whose telephone number is (571)272-3999. The examiner can normally be reached on Mon-Fri 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on (571)272-4001. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Hussein Elchanti

Jan. 25, 2005



SALEH NAJJAR
PRIMARY EXAMINER